(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

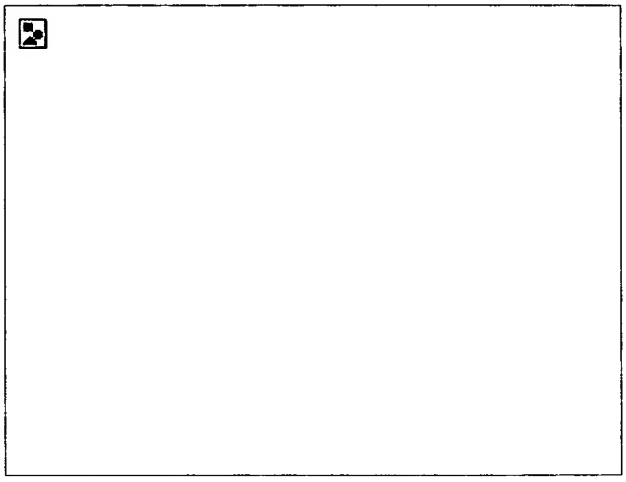
(11)Publication number: 1020030005675 A
(43)Date of publication of application: 23.01.2003

(21)Application number: 1020010041051
(22)Date of filing: 10.07.2001

(51)Int. Cl G06F 17/00

(71)Applicant: NITGEN CO., LTD.
(72)Inventor: JANG, U SEOK
KANG, YEONG MI
LEE, DONG WON

(54) SYSTEM AND METHOD FOR AUTHENTICATING WEB MODULE



(57) Abstract:

PURPOSE: A web module authentication system and method is provided to make a special server authenticate a web module, like an ActiveX control module, which is usually copied at a local PC and easily exchanged by a hacker in a conventional method.

CONSTITUTION: The method comprises several steps. A client executes a web browser(101), accesses a web server and requests the web server to offer a web service(102). A symmetric authentication key generation module of the web server generates the first symmetric authentication key (103), interposes the first symmetric authentication key in a web page(104), and transmits the web page to the client(105). Then the client requests a web module to offer the second symmetric authentication key on the first one before passing user data to the web module(106). A symmetric authentication key generation module of the client generates the second symmetric authentication key(107), and the generated second symmetric authentication key is compared with the first one(108). In a case that the second symmetric authentication key is identical to the first one, the client passes the user data to the web module, and starts to receive a web service(109).

Legal Status

Date of request for an examination (20010710)
Notification date of refusal decision ( )
Final disposal of an application (application)
Date of final disposal of an application ( )
Patent registration number ( )
Date of registration ( )

Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2003-0005675
G06F 17/00		(43) 공개일자	2003년01월23일
(21) 출원번호	10-2001-0041051		
(22) 출원일자	2001년07월10일		

(71) 출원인 (주)니트 젠
대한민국
137-860
서울 서초구 서초2동 1337-31 산학재단빌딩 18층

(72) 발명자 장우석
대한민국
135-779
서울특별시강남구도곡2동527번지도곡주공아파트31동308호

강영미
대한민국
137-070
서울특별시서초구서초동1324-7로뎀빌라304호

이동원
대한민국
449-846
경기도용인시수지읍풍덕천리700-1(1/18)현대아파트112동402호

(74) 대리인 박승민

(77) 심사청구 있음

(54) 출원명 웹모듈 인증 장치 및 방법

요약

본 발명은 웹서비스를 개시하기 전에 인증서버를 통해 웹모듈을 인증한 후 웹모듈의 인증이 확인된 경우에 한해서 서비스를 시작하는 웹모듈의 보안성을 증대시키기 위한 것으로서, 웹서버에는 클라이언트가 웹브라우저를 실행하여 웹서버에 접속하여 웹서비스를 요청하면 웹모듈 인증서버에 제1대칭인증키를 요청하고, 상기 웹모듈 인증서버의 대칭인증키 생성수단에서 생성되어 전송된 제1대칭인증키를 수신하는 통신수단; 웹페이지에 상기 제1대칭인증키를 삽입하여 클라이언트에 전송하는 수단이 포함되고, 상기 웹서버로부터의 요청에 의해서 대칭인증키를 생성하는 대칭인증키 생성수단을 포함하는 웹모듈 인증서버가 추가로 포함되며, 상기 클라이언트에는 클라이언트가 웹페이지를 전송받고 웹모듈에 이용자정보를 넘기기 전에 웹페이지에 삽입된 제1대칭인증키에 대한 제2대칭인증키를 생성하는 대칭인증키 생성수단; 상기 대칭인증키 생성수단에서 생성된 제2대칭인증키를 제1대칭인증키와 비교하여 제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈에 이용자인증 정보를 넘기고 웹서비스를 시작하는 인증수단이 포함되어 구성되는 웹모듈 인증 장치 및 방법이다.

대표도

도3

색인어

클라이언트, 웹서버, 웹모듈인증서버, 대칭인증키, 웹페이지, 통신, 웹모듈

명세서

도면의 간단한 설명

도1은 일반적인 웹서비스의 개요도.

도2a는 본 발명에 따른 시스템 구성도.

도2b는 본 발명에 따른 시스템 작업 흐름도.

도3은 본 발명의 실시예 시스템 구성도.

도4는 본 발명의 응용 실시예 시스템 구성도.

<도면부호의 설명>

서비스 웹페이지 생성(2), 웹모듈(4, 14), 웹페이지(12), 웹브라우저(16), 대칭인증키 생성모듈(18, 20), 통신모듈(22), 정보수신모듈(32), 클라이언트(100), 웹서버(200), 웹모듈 인증서버(300)

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 웹서비스를 개시하기 전에 인증서버를 통해 웹모듈을 인증한 후 웹모듈의 인증이 확인된 경우에 한해서 서비스를 시작하여, 웹모듈의 보안성을 증대시키는 장치 및 방법에 관한 것이다.

현재, 웹서비스는 HTML 페이지에서 태그(tag), 스크립트(script)를 이용하여 외부 모듈(ActiveX Control 등)을 호출하여 서비스를 하고 있다. 이는, HTML 페이지에서 태그, 스크립트를 사용하거나 ASP, JSP 등의 웹 스크립팅 언어를 사용하여 외부 모듈(COM, Win32 DLL, Java Bean 등)을 호출하는 방식으로 동작된다. 이하, 본 명세서에서는 웹서비스에 사용되는 ActiveX Control 등의 외부 모듈을 "웹모듈" 이라고 한다.

도1은 일반적인 웹서비스의 개요도이다. 동작은 클라이언트(100)에서 웹서버 (200)에 웹서비스를 요청하면, 웹서버(200)에서는 해당 HTML 문서를 제공한다. HTML 문서를 제공받은 클라이언트(100)의 웹브라우저에서는 웹모듈(4)을 호출하여 웹페이지 생성(2)을 하게 된다.

그러나, 상기의 종래방법에서 웹서비스에 사용되는 웹모듈들은 대개 사용자의 로컬 PC에 복사되어 사용되므로, 이들은 해커에 의해 쉽게 교체될 수 있다. 이와같이, 웹모듈이 해커에 의해 교체된 경우에는 이용자가 입력한 정보를 가로채거나 서비스 인증을 임의로 조작할 수 있는 문제점을 갖고 있다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 종래 방법의 문제점을 해결하기 위한 것으로서, 웹서비스에서 사용되는 웹모듈을 별도의 서버에서 인증하는 방식을 갖는 웹모듈 인증 장치 및 방법을 제공함에 있다.

웹서비스를 개시하기 전에 웹모듈 인증서버를 통해 웹모듈을 인증한 후 웹모듈의 인증이 확인된 경우에 한해서 서비스를 시작하므로, 해킹에 의해서 교체되거나 기타 변경된 모듈인 경우에는 서비스가 이루어지지 않게 된다. 한편, 웹모듈 인증서버측에서는 고객의 웹브라우저에 광고를 비롯한 다양한 정보의 제공이 가능하므로, 그에 따른 광고효과도 가져올 수 있다.

발명의 구성 및 작용

<발명의 개요>

본 발명은 전체적으로 웹서버에 접속하여 웹서비스를 요청하는 클라이언트의 웹브라우저와, 웹브라우저로부터 웹서비스를 요청받으면 웹서비스를 수행하는 웹페이지를 클라이언트로 제공하는 웹서버로 구성된다. 본 발명에 따른 장치의 구성을 도2a를 참조하여 설명한다.

본 발명은 기본적으로, 웹서버(200)에 저장된 웹페이지(12)를 클라이언트 (100)에서 제공받고, 웹모듈(14)을 이용하여 웹페이지(12)에 의한 웹서비스를 제공받는 시스템에서 이루어진다.

상기 웹서버(200)는, 클라이언트(100)의 웹브라우저(16)로부터 통신모듈(22)을 통해 웹서비스 요청을 받으면 제1대칭인증키를 생성하는 대칭인증키 생성모듈 (18)과, 상기 대칭인증키 생성모듈(18)에서 생성된 제1대칭인증키를 웹페이지(12)에 삽입하여 클라이언트(100)에 전송하는 수단이 포함된다.

상기 웹서버(200)로부터 웹페이지(12)가 제공되면, 클라이언트(100)에서는 웹페이지(12)를 전송받고 웹모듈(14)에 이용자정보를 넘기기 전에 웹페이지(12)에 삽입된 제1대칭인증키에 대해 대칭인증키 생성모듈(20)로부터 제2대칭인증키를 생성한다. 그리고, 대칭인증키 생성모듈(20)이 제2대칭인증키를 생성하면 제1대칭인증키와 제2대칭인증키를 비교한 후 제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈(14)에 이용자인증정보를 넘기고 웹서비스를 시작하는 인증수단이 포함된다.

상기와 같이 구성되는 시스템상의 작업 흐름을 도2b를 중심으로 도2a를 참조하여 설명한다.

본 발명에 따른, 웹서버(200)에 저장된 웹페이지(12)를 클라이언트(100)에서 제공받고, 클라이언트(100)의 웹모듈(14)을 이용하여 웹페이지(12)에 의한 웹서비스를 제공받는 시스템상의 흐름을 단계별로 설명하면 다음과 같다.

먼저, 클라이언트(100)가 웹브라우저를 실행[101]하여 웹서버(200)에 접속하여 통신모듈(22)을 통해 웹서비스를 요청하면[102], 웹서버(200)에서는 대칭인증키 생성모듈(18)에서 제1대칭인증키를 생성[103]하고, 생성된 제1대칭인증키를 웹페이지에 삽입[104]하여 클라이언트(100)로 전송하는 단계[105]가 수행된다.

웹페이지(12)를 전송받은 클라이언트(100)에서는 웹모듈(14)에 이용자정보를 넘기기 전에, 웹페이지(12)에 삽입되어 전송된 제1대칭인증키에 대한 제2대칭인증키를 웹모듈(14)에 요청하는 단계[106]가 수행되며,

대칭인증키 생성모듈(20)에서 제2대칭인증키를 생성하면[107], 생성된 제2대칭인증키와 제1대칭인증키를 비교하여 일치하는지 확인하는 단계[108]가 수행된다.

비교 후, 제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈(14)에 이용자 인증정보를 넘기고 웹서비스를 시작하는 단계[109]로 이루어진다.

<구체화된 실시예>

상기에서 설명한 도2a, 2b의 개념은 도3과 같이 별도의 웹모듈 인증서버에 의해 구현이 가능해진다.

도3에서 보는 바와 같이, 본 발명의 실시예는 웹서버(200)에 접속하여 웹서비스를 요청하는 클라이언트(100)의 웹브라우저(16)와, 웹브라우저(16)로부터 웹서비스를 요청받으면 웹서비스를 수행하는 웹페이지(12)를 클라이언트(100)로 제공하는 웹서버(200), 상기 웹서버(200)로부터의 대칭인증키 요청에 의해서 대칭인증키를 생성하는 대칭인증키 생성모듈(18)을 포함하는 웹모듈 인증서버(300)가 추가로 포함되어 구성된다.

여기서, 상기 웹서버(200)에는, 클라이언트(100)가 웹브라우저(16)를 실행하여 웹서버(200)에 접속하여 웹서비스를 요청하면 웹모듈 인증서버(300)에 제1대칭인증키를 요청하고, 상기 웹모듈 인증서버(300)의 대칭인증키 생성모듈(18)에서 제1대칭인증키가 생성되어 전송되며, 전송된 제1대칭인증키를 수신하는 통신모듈 (22)과 웹페이지(12)에 상기 제1대칭인증키를 삽입하여 클라이언트(100)에 전송하는 수단이 포함된다.

웹서버(200)로부터 웹페이지(12)를 제공받은 상기 클라이언트(100)에는, 웹모듈(14)에 이용자정보를 넘기기 전에 웹페이지(12)에 삽입된 제1대칭인증키에 대한 제2대칭인증키를 생성하는 대칭인증키 생성모듈(20)과 대칭인증키 생성모듈(20)에서 제2대칭인증키를 생성하면 제1대칭인증키와 제2대칭인증키를 비교한 후 제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈(14)에 이용자인증 정보를 넘기고 웹서비스를 시작하는 인증수단이 포함된다.

상기에서 설명한 바와 같이, 본 실시예에 따르면 웹서버(200)에는 웹모듈 인증서버(300)에 대칭인증키를 요청하고 수신하는 통신모듈(22)이 포함되며, 웹모듈 인증서버(300)에는 대칭인증키 생성함수에 의해 대칭인증키를 생성하는 대칭인증키 생성모듈(18)이 포함되는 것을 알 수 있다.

상기와 같이 구성되는, 본 발명의 시스템의 흐름을 도3을 참조하여 설명한다.

클라이언트(100)가 웹브라우저(16)를 실행하여 웹서버(200)에 접속하여 웹서비스를 요청하면[201], 웹서버(200)에서는 웹모듈 인증서버(300)에 제1대칭인증키를 요청하는 단계[202]가 수행된다.

웹모듈 인증서버(300)의 대칭인증키 생성모듈(18)에서는 대칭키 생성함수를 통해 제1대칭인증키를 생성[203]한 후, 웹서버(200)에 전송하는 단계[204]가 수행된다.

제1대칭인증키를 전송받은 웹서버(200)에서는 웹페이지(12)에 제1대칭인증키를 삽입하여 클라이언트(100)에 전송하는 단계[205]가 수행되며,

클라이언트(100)에서는 웹페이지(12)를 전송받고 웹모듈(14)에 이용자정보를 넘기기 전에, 웹페이지(12)에 삽입된 제1대칭인증키에 대한 제2대칭인증키를 웹모듈(14)에 요청한다.

웹서버(200)로부터 제공받은 서비스 웹페이지에서는 웹모듈(14)에 요청하여 대칭인증키 생성모듈(20)에서 생성된 제2대칭인증키를 제1대칭인증키와 비교하여 일치하는지 확인하는 단계[206]가 수행되며,

제1대칭인증키와 제2대칭인증키가 일치하여 인증이 확인되면, 웹모듈(14)에 이용자인증 정보를 넘기고 웹서비스를 시작하는 단계[207]로 이루어진다.

여기서, 좀더 상세히 설명하면, 웹서버(200)에서 웹모듈 인증서버(300)로 요청한 대칭인증키가 A라면, 웹모듈 인증서버(300)에서 대칭키 생성함수를 통해 생성된 대칭인증키는 A와 A에 대한 대칭인증키 B가 생성된다. 생성된 대칭인증키는 웹서버(200)의 통신모듈(22)로 전송된 후 웹페이지(12)에 삽입되어 클라이언트(100)로 전송된다. 클라이언트(100)에서는 웹서버(200)로부터 대칭인증키가 내장된 서비스 웹페이지를 제공받는데, 여기에는 대칭인증키 A와 내장된 대칭인증키 B가 있다. 다음으로, 클라이언트(100)에서 대칭인증키 A에 대한 대칭인증키의 요청에 따라 클라이언트(100)에 제공된 웹모듈(ActiveX Control 등, 14)에서는 대칭인증키 생성모듈(20)로부터 A에 대한 대칭인증키 B'를 제공받는다. 제공받은 대칭인증키 B'와 웹모듈 인증서버(300)로부터 생성되어 전송된 대칭인증키 B와의 일치여부를 확인한 후, 일치여부가 확인되면 웹모듈(14)로 이용자 인증정보를 넘기고 웹서비스를 시작하게 된다.

<응용 실시예>

본 발명의 웹모듈 인증장치는 이용자에게 정보 푸시서비스(Push Service)를 수행하는 모델에 응용될 수 있다. 이에 따른, 시스템 구성을 도4를 참조하여 설명한다.

도4에서 보는 바와 같이, 웹모듈 인증장치를 이용하여 이용자에게 정보 푸시서비스를 수행하는 시스템에서, 클라이언트(100)는 웹서버(200)에 웹서비스 요청을 할 때에 클라이언트(100)의 IP주소를 웹서버(200)로 전송한다. 클라이언트(100)의 IP주소를 전송받은 웹서버(200)에서는 웹모듈 인증서버(300)의 대칭인증키 생성모듈(18)에 대칭인증키를 요청할 때에, 클라이언트(100)의 IP주소도 함께 전송한다.

웹모듈 인증서버(300)에서는 클라이언트(100)의 IP주소를 전송받아 저장해 놓고, 이 IP주소에 정보를 푸시서비스하게 된다. 푸시서비스된 정보를 수신하기 위해 클라이언트(100)에는 정보 수신모듈(32)이 추가로 포함된다.

상기와 같이 구성되는, 본 발명에 따른 웹모듈 인증장치를 이용하여 이용자에게 정보푸시서비스를 수행하는 시스템상의 흐름을 도4를 참조하여 설명한다.

도4에서 보는 바와 같이, 먼저, 클라이언트(100)가 웹서버(200)에 웹서비스 요청을 할 때에, 클라이언트(100)는 자신의 IP주소를 웹서버(200)에 함께 전달한다 [302].

클라이언트(100)의 IP주소를 전송받은 웹서버(200)의 통신모듈(22)에서는 웹모듈 인증서버(300)에 제1대칭인증키를 요청할 때에, 클라이언트(100)로부터 전송받은 클라이언트(100)의 IP주소를 웹모듈 인증서버(300)에 함께 전송한다[304].

웹모듈 인증서버(300)의 대칭인증키 생성모듈(18)에서는 제1대칭인증키 생성 [308]과 클라이언트(100)의 IP주소를 전송받아 저장해 놓고, 이 IP주소에 정보를 푸시서비스하는 단계[306]가 수행된다. 웹모듈 인증서버(300)에서의 정보 푸시서비스는 클라이언트(100)의 정보 수신모듈(32)로 전송된다[312]. 또한, 대칭인증키 생성모듈(18)에서 대칭함수를 통해 생성된 제1대칭인증키는 앞에서 설명한 바와 같이, 웹서버(200)의 통신모듈(22)로 전송된다[310].

이와같이, 본 발명에서 웹모듈 인증서버(300)는 클라이언트(100)의 IP주소를 저장해 놓고 있다가, 광고나 정보를 직접 푸시하는 푸시서비스를 수행한다. 이와같이, 본 발명의 응용 실시예에서 웹모듈 인증서버(300)는 웹모듈 인증기능 이외에 ASP (Application Service Provider) 서버로서의 역할도 하는 것이다.

또한, 클라이언트(100)의 정보수신모듈(32)은, 예를 들어 프로그램 설치시 자동으로 설치될 수 있으며 백그라운드에서 푸시서비스를 위해 동작하다가 정보를 받으면 정보를 이용자에게 제공하는 역할을 수행한다.

발명의 효과

이상에서와 같이, 본 발명의 웹모듈 인증 장치 및 방법에 따르면, 웹모듈의 해킹을 웹모듈 인증서버의 인증을 통해 막을 수 있으며, 웹모듈 인증 ASP 서비스를 창출할 수 있는 효과를 얻을 수 있다. 또한, 웹모듈 인증 ASP에서는 고객의 웹페이지에 광고를 비롯한 기타 정보를 제공할 수 있으며, 웹모듈 인증을 제품 개발업체가 하는 경우에 제품에 대한 업그레이드 정보나 신제품 및 회사의 고객정보를 쉽게 고객에게 전달할 수 있는 효과를 얻을 수 있다. 또한, 응용프로그램의 기본 UI가 웹브라우저를 이용하여 HTML 페이지로 구성되는 경우, OEM 업체에 대한 지원이 용이한 효과를 얻을 수 있다.

(57) 청구의 범위

청구항 1.

웹서버에 접속하여 웹서비스를 요청하는 클라이언트의 웹브라우저와, 웹브라우저로부터 웹서비스를 요청받으면 웹서비스를 수행하는 웹페이지를 클라이언트로 제공하는 웹서버로 구성되어, 웹서버에 저장된 웹페이지를 클라이언트에서 제공받고 웹모듈을 이용하여 웹페이지에 의한 웹서비스를 제공받는 시스템에 있어서,

상기 웹서버에는, 웹브라우저로부터 웹서비스 요청을 받으면 제1대칭인증키를 생성하는 웹서버의 대칭인증키 생성수단; 상기 대칭인증키 생성수단에서 생성된 제1대칭인증키를 웹페이지에 삽입하여 클라이언트에 전송하는 수단이 포함되고,

상기 클라이언트에는, 클라이언트가 웹페이지를 전송받고 웹모듈에 이용자정보를 넘기기 전에 웹페이지에 삽입된 제1대칭인증키에 대한 제2대칭인증키를 생성하는 대칭인증키 생성수단; 상기 대칭인증키 생성수단에서 생성된 제2대칭인증키를 제1대칭인증키와 비교하여 제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈에 이용자인증 정보를 넘기고 웹서비스를 시작하는 인증수단이 포함되는 것을 특징으로 하는, 웹모듈 인증장치.

청구항 2.

웹서버에 접속하여 웹서비스를 요청하는 클라이언트의 웹브라우저와, 웹브라우저로부터 웹서비스를 요청받으면 웹서비스를 수행하는 웹페이지를 클라이언트로 제공하는 웹서버로 구성되어, 웹서버에 저장된 웹페이지를 클라이언트에서 제공받고 웹모듈을 이용하여 웹페이지에 의한 웹서비스를 제공받는 시스템에 있어서,

상기 웹서버로부터의 요청에 의해서 대칭인증키를 생성하는 대칭인증키 생성수단을 포함하는 웹모듈 인증서버가 추가로 포함되며,

상기 웹서버에는, 클라이언트가 웹브라우저를 실행하여 웹서버에 접속하여 웹서비스를 요청하면 웹모듈 인증서버에 제1대칭인증키를 요청하고, 상기 웹모듈 인증서버의 대칭인증키 생성수단에서 생성되어 전송된 제1대칭인증키를 수신하는 통신수단; 웹페이지에 상기 제1대칭인증키를 삽입하여 클라이언트에 전송하는 수단이 포함되고,

상기 클라이언트에는, 클라이언트가 웹페이지를 전송받고 웹모듈에 이용자정보를 넘기기 전에 웹페이지에 삽입된 제1대칭인증키에 대한 제2대칭인증키를 생성하는 대칭인증키 생성수단; 상기 대칭인증키 생성수단에서 생성된 제2대칭인증키를 제1대칭인증키와 비교하여 제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈에 이용자인증 정보를 넘기고 웹서비스를 시작하는 인증수단이 포함되는 것을 특징으로 하는, 웹모듈 인증장치.

청구항 3.

청구항 2에서,

클라이언트가 웹서버에 웹서비스 요청을 할 때에 클라이언트의 IP주소를 웹서버에 전달하는 수단,

웹서버가 웹모듈 인증서버의 대칭인증키 생성수단에 대칭인증키를 요청할 때에, 클라이언트로부터 전달받은 클라이언트의 IP주소를 함께 전달하는 수단,

웹모듈 인증서버가 IP주소를 전달받아 저장해 놓고, 이 IP주소에 정보를 푸시서비스하는 수단,

클라이언트가 웹모듈 인증서버로부터 푸시되는 정보를 수신하는 정보수신 수단이 추가로 포함되는 것을 특징으로 하는, 웹모듈 인증장치.

청구항 4.

웹서버에 저장된 웹페이지를 클라이언트에서 제공받고 웹모듈을 이용하여 웹페이지에 의한 웹서비스를 제공받는 시스템에 있어서,

클라이언트가 웹브라우저를 실행하여 웹서버에 접속하여 웹서비스를 요청하면, 웹서버에서는 제1대칭인증키를 생성하고 이 제1대칭인증키를 웹페이지에 삽입하여 클라이언트에 전송하는 단계,

클라이언트가 웹페이지를 전송받고 웹모듈에 이용자정보를 넘기기 전에 웹페이지에 삽입된 제1대칭인증키에 대한 제2대칭인증키를 웹모듈에 요청하는 단계,

생성된 제2대칭인증키를 제1대칭인증키와 비교하여 일치하는지 확인하는 단계,

제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈에 이용자인증 정보를 넘기고 웹서비스를 시작하는 단계로 이루어지는, 웹모듈 인증방법.

청구항 5.

웹서버에 저장된 웹페이지를 클라이언트에서 제공받고 웹모듈을 이용하여 웹페이지에 의한 웹서비스를 제공받는 시스템에 있어서,

클라이언트가 웹브라우저를 실행하여 웹서버에 접속하여 웹서비스를 요청하면, 웹서버에서는 웹모듈 인증서버에 제1대칭인증키를 요청하는 단계,

웹모듈 인증서버가 인증키 생성함수에 의해 제1대칭인증키를 생성하여 웹서버에 전송하는 단계,

웹서버가 웹페이지에 제1대칭인증키를 삽입하여 클라이언트에 전송하는 단계,

클라이언트가 웹페이지를 전송받고 웹모듈에 이용자정보를 넘기기 전에 웹페이지에 삽입된 제1대칭인증키에 대한 제2대칭인증키를 웹모듈에 요청하는 단계,

생성된 제2대칭인증키를 제1대칭인증키와 비교하여 일치하는지 확인하는 단계,

제1대칭인증키와 제2대칭인증키가 일치하면 웹모듈에 이용자인증 정보를 넘기고 웹서비스를 시작하는 단계로 이루어지는, 웹모듈 인증방법.

청구항 6.
청구항 5에서,

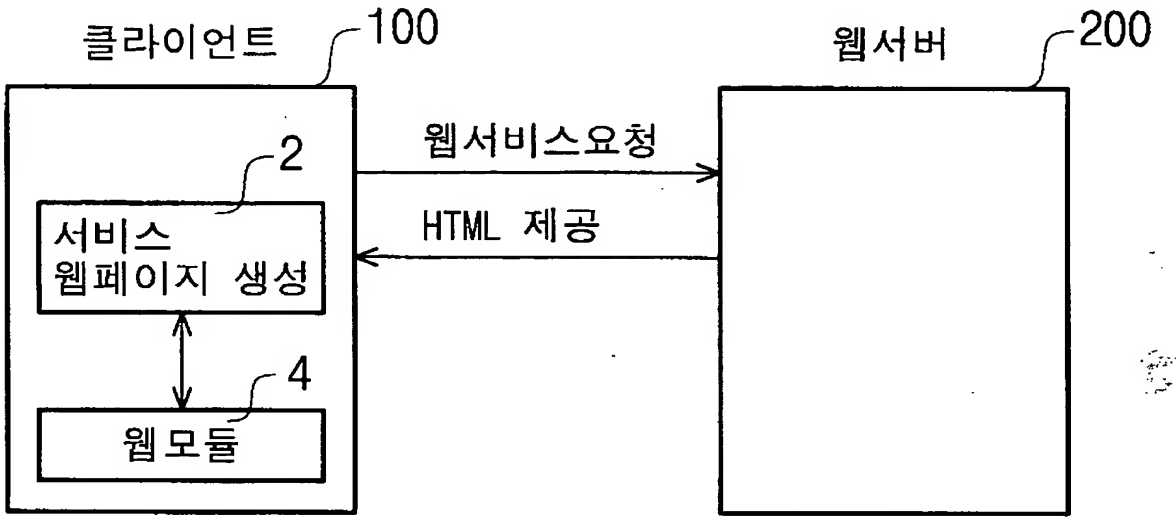
클라이언트가 웹서버에 웹서비스 요청을 할 때에, 클라이언트는 클라이언트 자신의 IP주소를 웹서버에 전달하는 단계,

웹서버가 웹모듈 인증서버에 제1대칭인증키를 요청할 때에, 웹서버는 클라이언트로부터 전달받은 클라이언트의 IP주소를 웹모듈 인증서버에 전달하는 단계,

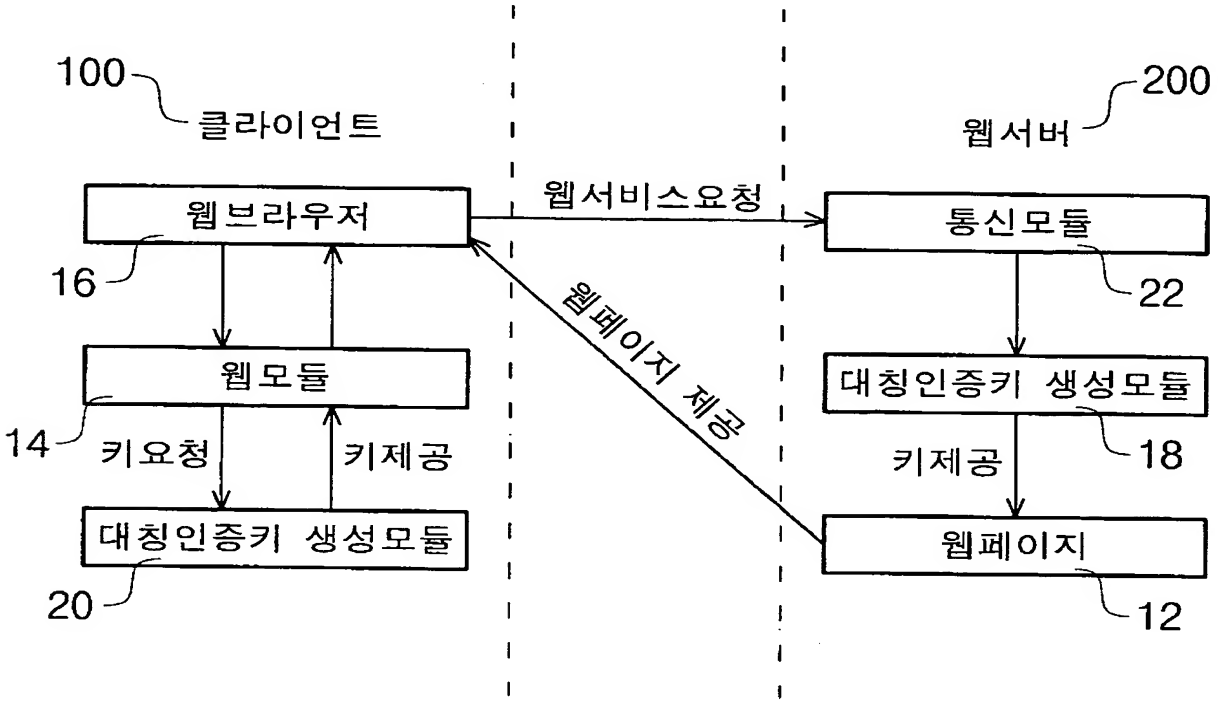
웹모듈 인증서버가 IP주소를 전달받아 저장해 놓고, 이 IP주소에 정보를 푸시서비스하는 단계가 추가로 포함되는, 웹모듈 인증방법.

도면

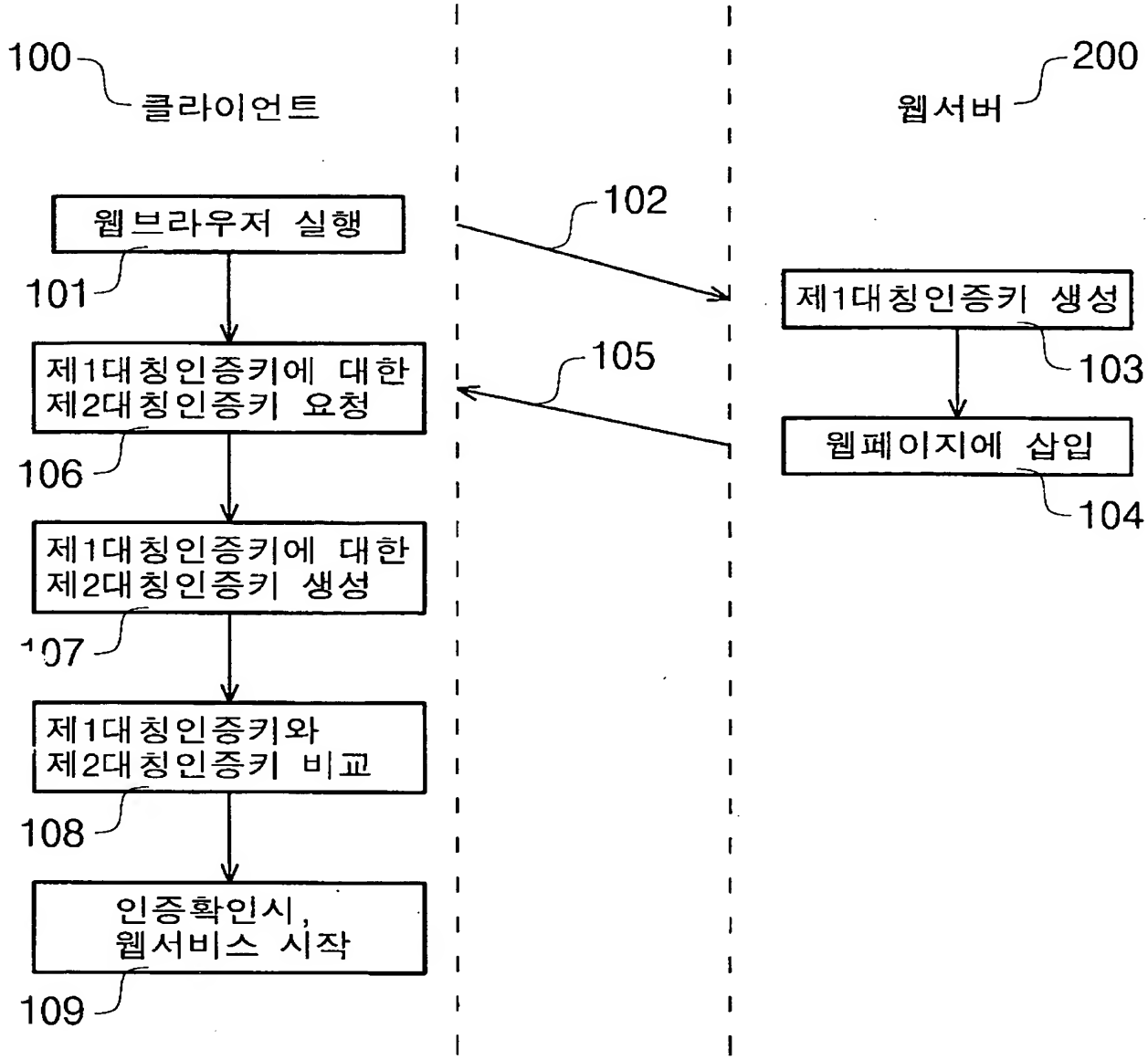
도면 1



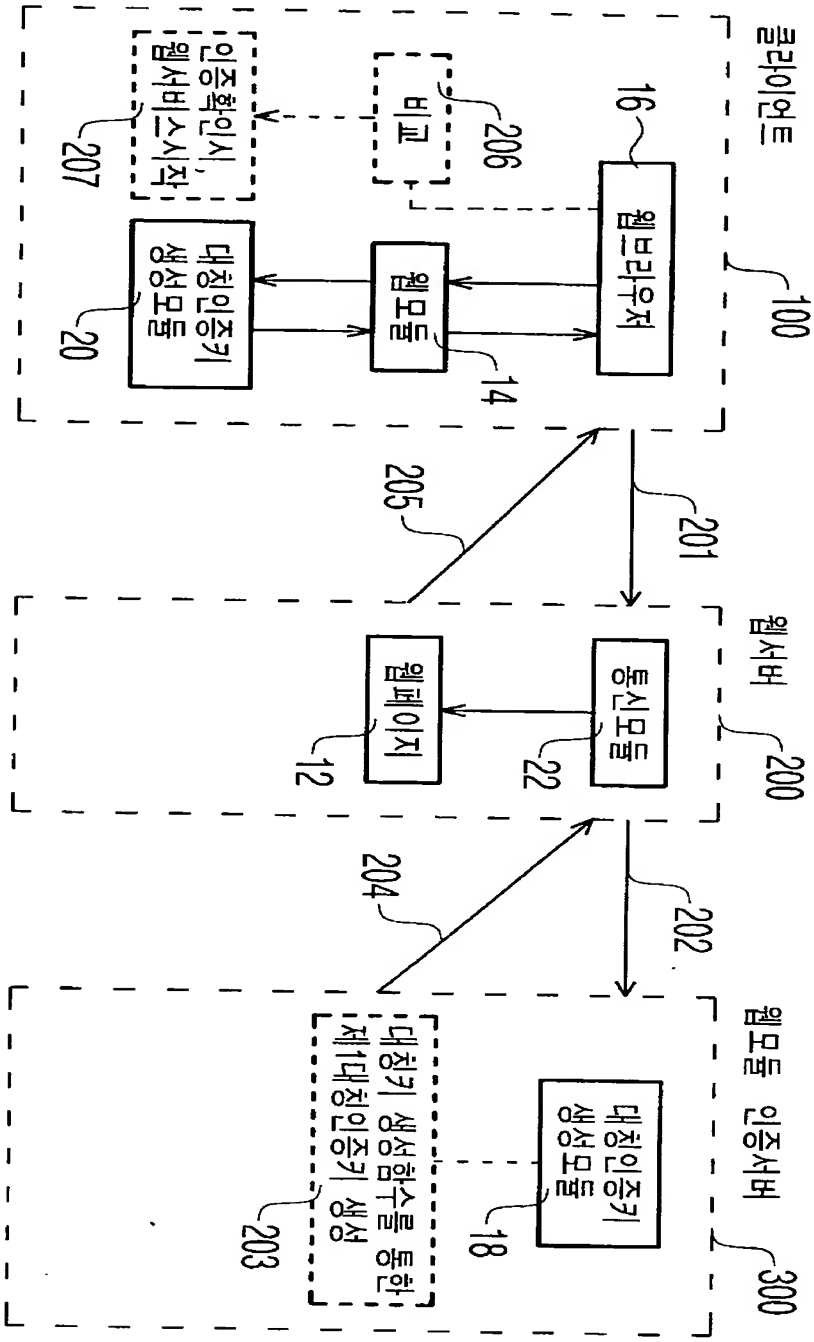
도면 2a


100
클라이언트
200
웹서버
웹브라우저
웹서비스요청
통신모듈
16
22
웹페이지 제공
웹모듈
대칭인증키 생성모듈
14
키요청
키제공
키제공
18
대칭인증키 생성모듈
웹페이지
20
12

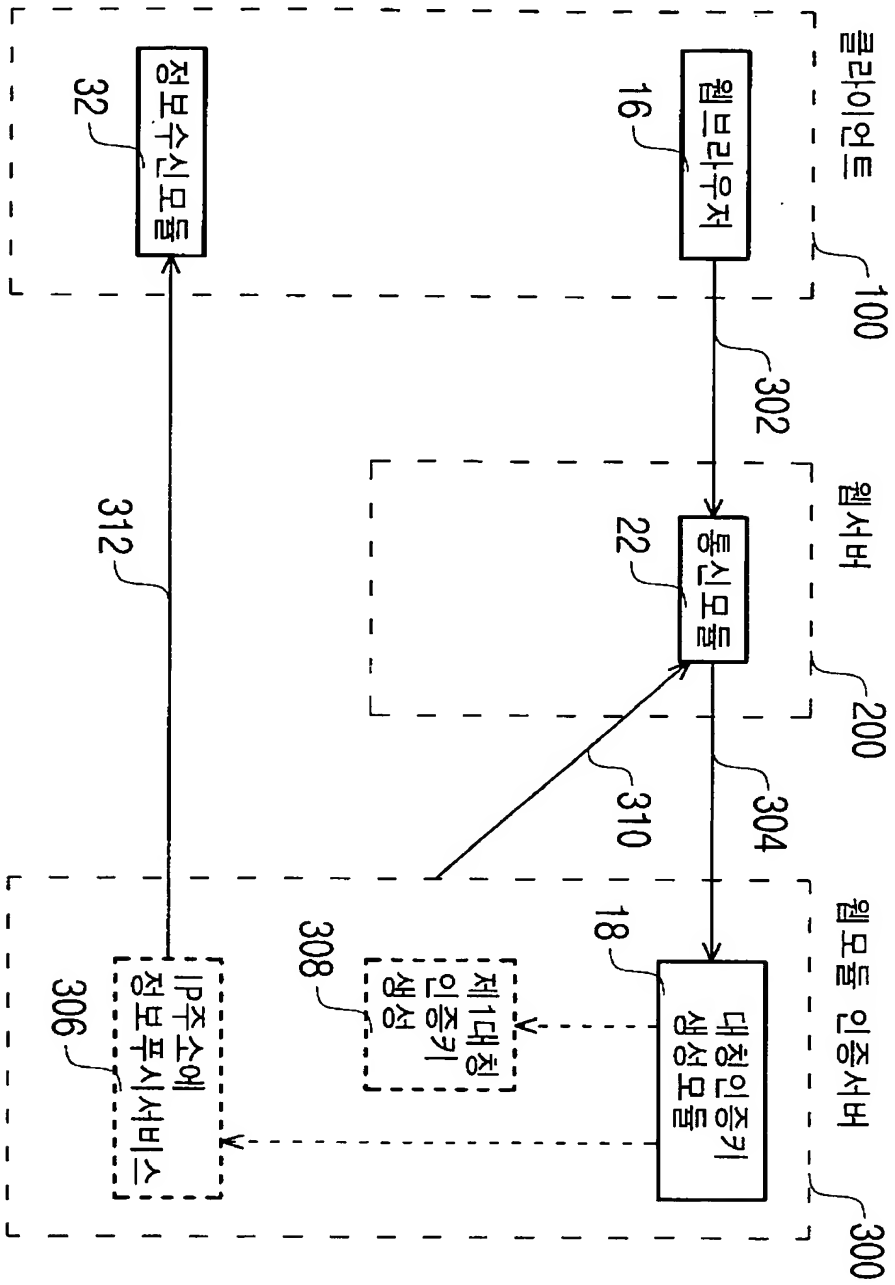
도면 2b


100
클라이언트
200
웹서버
웹브라우저 실행
101
102
제1대칭인증키 생성
103
제1대칭인증키에 대한
제2대칭인증키 요청
105
106
웹페이지에 삽입
104
제1대칭인증키에 대한
제2대칭인증키 생성
107
제1대칭인증키와
제2대칭인증키 비교
108
인증확인시,
웹서비스 시작
109

도면 3


클라이언트
100
웹브라우저
16
웹모듈
14
대칭인증키 생성모듈
20
비교
206
인증확인시, 웹서비스시작
207
205
201
웹서버
200
웹페이지
12
통신모듈
22
204
202
웹모듈 인증서버
300
대칭인증키 생성모듈
18
대칭키 생성함수를 통한 제1대칭인증키 생성
203

도면 4


클라이언트
100
웹브라우저
16
정보수신모듈
32
302
웹서버
200
통신모듈
22
310
304
312
웹모듈 인증서버
300
대칭인증키
생성모듈
18
제1대칭
인증키
생성
308
IP주소에
정보푸시서비스
306